

REMARKS/ARGUMENTS

In the Office communication of December 13, 2005, the Examiner stated that Amendment C was not fully responsive because the newly submitted claims were not addressed.

Amendment C added new claims 37-41. Claims 37-38 are dependent on claim 1, and as noted in the Amendment, are submitted as patentable for at least the reasons discussed with respect to independent claim 1.

Applicant respectfully submits that claim 39 is patentable over the cited references, including Cheriton et al., Romig et al., and Smith et al., which do not show or suggest monitoring statistics associated with aggregate filters, creating a network flow for packets passing through a first aggregate filter, sending a network flow summary corresponding to the network flow to a flow analyzer operable to analyze the network flow, and refining the first aggregate filter based on the analyzed flow.

As discussed in the Remarks/Arguments section of Amendment C, the Cheriton et al. reference cited discloses datagram transmission over virtual circuits. The invention of Cheriton et al. is directed to providing support for a wide range of network transmission speeds and a wide variety of source traffic behavior, while maintaining compatibility with existing network protocols and applications. The Cheriton et al. PCT application does not show or suggest sending a network flow summary to a flow analyzer operable to analyze the network flow or refining an aggregate filter based on the analyzed flow.

The Romig et al. and Smith references were also discussed in Amendment C (see pages 10-11). Romig et al. describe flow logs which capture a record of flows as they are removed from a flow cache. Romig et al. created a suite of tools to record and analyze flow logs. The flow logs may be used, for example, after an intrusion is reported to reach the captured flow logs and determine when the initial attack occurred and what network traffic ensued from the victim host after the intrusion. The intrusion detection tools used by Romig et al. read through a set of previously captured flow logs (e.g., for a 24-hour period) and report on host and port scans. Other tools are used to investigate the intrusion more thoroughly (e.g., using flow-search and

flow-print to extract specific records). The system is used to analyze data after an attack and does not provide for analysis as the attack is occurring. There is no monitoring of statistics or a filter generated to limit data coming into a network.

The Smith et al. reference teaches a firewall that works with intrusion detection software to automatically cause a set of firewalls to dynamically change security policy for individual attack activity. The gateway device acts as an autonomous system in policing activity of illegal hackers so that the blocking of unwanted inbound traffic is performed at the gateway network, rather than a network device within a corporate network. Thus, the data entering the gateway is policed. Applicant's invention, as set forth in claim 39, creates a network flow for packets passing through a first aggregate filter and sends this data to a flow analyzer. This allows for progressive refinement of the aggregate filter to identify detailed characteristics of packets involved in an attack or failure.

Accordingly, claim 39 is submitted as patentable over Cheriton et al., Romig et al., Smith et al, and the other references of record.

Claims 40 and 41, depending directly from claim 39, are submitted as patentable for at least the reasons discussed above with respect to claim 39.

For the foregoing reasons and those set forth in Amendment C, Applicant believes that all of the pending claims are in condition for allowance and should be passed to issue. If the Examiner feels that a telephone conference would in any way expedite the prosecution of the application, please do not hesitate to call the undersigned at (408) 399-5608.

Respectfully submitted,



Cindy S. Kaplan
Reg. No. 40,043

P.O. Box 2448
Saratoga, CA 95070
Tel: 408-399-5608
Fax: 408-446-8691